APPENDIX A
Impact of Work-at-Home on Personnel Management Issues

1. Job Descriptions. Changes to job descriptions normally should not be required, unless the work-at-home arrangement changes the actual position duties or the position description is not up-to-date. Supervisors should carefully specify the employee's official duties by defining Work at Home requirements as narrowly and precisely as possible. Minor modifications in the job description may be needed to reflect the supervisory controls or work environment factors.

2. TAPES Objectives. Generally changes to performance objectives should not be necessary.

3. Work Schedules. Local work schedule policies will apply to Work at Home participants.

4. Leave. The policies for requesting annual leave, sick leave, or leave without pay remain unchanged. The employee is responsible for requesting leave in advance from the supervisor and annotating leave usage on the time sheet.

5. Time and Attendance. Supervisors must report time and attendance to ensure that employees are paid only for work performed and that absences from scheduled tours of duty are accounted for correctly. Local procedures will be established for documenting work at home on official time records.

6. Administrative Leave, Dismissals, Emergency Closings. Although a variety of circumstances may affect individual situations, the principles governing administrative leave, dismissals, and closings remain unchanged. The ability to conduct work (and the nature of any impediments), whether at home or at the office, determines when an employee may be excused from duty. For example, if the employee is working at home and the main office closes, normally the flexiplace employee will continue working at home. However, if the employee's electricity fails while working at home, the supervisor may grant administrative leave. When an employee knows in advance of a situation that would preclude working at home, either time in the office or leave should be scheduled.

7. Pay entitlements. All pay, special salary rates, leave and travel entitlements will be based on the employee's official duty station.

a. Premium Pay. The normal rules apply for night differentials, and Sunday and holiday pay whether work is accomplished at the conventional or home worksite. Official work schedules determine the entitlement to premium pay.

b. Fair Labor Standards Act (FLSA). The existing rules governing overtime also apply to Work at Home arrangements. Overtime is time worked at official duties in excess of the scheduled tour of duty that is ordered and approved by the supervisor. It is the responsibility of the supervisor to regulate and control the use of overtime. Employees are responsible for requesting, in advance, approval to work in excess of their normal hours of duty. This is particularly important when employees are working at home without direct supervisory oversight. Managers must ensure that only the work for which it intends to make payment is performed. Since the supervisor is not on the scene, s/he must provide clear directions to participating employees. Supervisors must communicate work rules and monitor work activity. Non-exempt flexiplace employees who work in excess of the hours approved by managers to receive compensation should be removed from the program. (Employees working under flexible work schedules that include credit hours may elect to work credit hours on work at home days in accordance with local policies.)

8. Liability and Workers' Compensation. Any Government exposure to liability would be covered under the Military Personnel and Civilian Employees Claims Act, the Federal Tort Claims Act, or the Federal Employees Compensation Act. Work at Home participants whose injury claims are accepted by the Office of Workers' Compensation Programs may qualify for continuation of pay or workers' compensation for an on-the-job injury or occupational illness. The supervisor's signature on the request for compensation attests only to what the supervisor can reasonably know, whether the event occurred at the conventional or home work site. Under normal circumstances, supervisors are often not present when an employee sustains an injury. In all situations, an employee bears responsibility for informing his or her immediate supervisor of an injury at the earliest time possible. The employee must also provide details to the Department of Labor when filing a claim. Supervisors must ensure that claims of this type are brought to the attention of the office providing workers' compensation services.

9. Home Utility Expenses. The Government does not pay home utility costs associated with working at home. Potential savings to the employee resulting from reduced commuting, meals, etc., may offset any incidental increase in utility expenses. Exceptions apply only where the personal expense directly benefits the government, e.g., business related long distance calls on the employee's personal phone or a separate telephone line when warranted.

10. Tax Benefits. Generally, an employee who uses a portion of his or her home does not qualify for any Federal tax deductions. However, employees should consult a tax advisor or the Internal Revenue Service for information on tax laws and interpretations that address their specific circumstances.

APPENDIX B

Government Owned Property

1. Government-owned property, including computers and other telecommunications equipment, may be removed from LRD activities, if authorized, and used by employees in their private residence provided the equipment is used only for official business. The government must retain ownership and control of hardware, software, and data. In these situations, the government is responsible for maintenance, repair, and replacement of such equipment. The employee must notify his/her supervisor immediately following a malfunction of government-owned equipment. Normally loaner equipment will not be available while the failed equipment is being repaired. If repairs are extensive, the employee may be asked to report to the main office until equipment is usable.

2. Each organization must establish its own policy on purchase and installation of equipment. Transfer of computers, printers, modems and other data processing equipment from the office to the home residence and back is determined by the organization, but normally organizations will make transport of equipment an individual responsibility. Property accountability will be maintained in accordance with ER 700-1-1, USACE Supply Policies and Procedures.

3. Only hardware/software procured by the Federal government and authorized by an approving official for the alternate work site will be installed on government owned computers. Under no circumstances will employees add non-government owned or unauthorized hardware or software to the government owned home computer workstation. Government approved anti-virus software will be installed and routinely run on all computers processing government information. This applies to both government and non-government computers.

APPENDIX C

Security Issues

Army Regulation 25-1, The Army Information Resources Management Program, Chapter 5, contain policy and procedures for processing government information at locations other than at the normal work site. If an employee is approved for the work at home program the following procedures will apply:

a. All computers used for offsite processing of government information must be accredited in accordance with AR 380-19, Information Systems Security, by the Designated Approving Authority (DAA) prior to initiation of offsite processing. Computers may be accredited under blanket documentation instruments providing they have like risks, threats, and countermeasures. This applies to both government and non-government computers.

b. The employee must receive a systems and information security briefing from the Information System Security Officer (ISSO) or Information System Security Manager (ISSM) once the accreditation process is complete and before data access is granted.

c. System use and data access is restricted to business related activities only and to the authorized Corps employee.

d. The system administrator or network security officer will conduct daily audit trails of the Local Area Network. If any unauthorized use or misuse of privileges are detected the employee work-at-home privileges may be immediately revoked indefinitely.

e. Security of government equipment located at the employee's home is the employee’s responsibility. The employee will be held accountable for damages, theft, or destruction of all government owned equipment if found negligent. The Government will not be liable for damages to an employee's personal or real property during the course of performing official duties or while using Government information technology resources in the employee's residence, except to the extent the Government is held liable by Federal Tort Claims Act claims or claims arising under the Military Personnel and Civilian Employees' Claims Act.

f. Only authorized hardware and software will be attached or loaded on government equipment. Requests for any changes or modifications to existing hardware or software will require reaccreditation approval through the Information Systems Security Manager.

g. The supervisor is responsible for ensuring that appropriate security control measures are in place prior to the approval of a work-at-home status. The level of control and protection

will be commensurate with the maximum sensitivity of the information present in the system and will provide the most restrictive control measures required by the data to be handled. This includes personnel, physical, administrative, and configuration controls.

1) Privacy Act, Sensitive or Classified Data. Decisions regarding the proper use and handling of sensitive data, as well as records subject to the Privacy Act, are delegated to individual supervisors who permit employees to work at home. Off-site access to sensitive data may be permitted provided Information Systems Security manager (ISSM) and the Information Systems Security Officer (ISSO) certify the adequacy of security for such access. Classified data may not be removed from employees' official work sites to off-site locations.

2) Care must be taken to ensure that records subject to the Privacy Act and sensitive non-classified data are not disclosed to anyone except to those who are authorized access to such information in order to perform their duties. Organizations allowing employees to access records subject to the Privacy Act from a remote work site must maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the records. When records subject to the Privacy Act are maintained or used by employees working at home or at other remote locations, installations should revise the appropriate record system notices to indicate that the off-site system location is authorized.

h. The employee will ensure all hardware, software, documentation, and all data handled by the Automated Information System (AIS) is protected to prevent unauthorized intentional or (unintentional) disclosure, destruction, or modification. The employee will document the security procedures for safeguarding the system and the data in the accreditation document.